GRAPHICAL PASSWORD AUTHENTICATION USING PASS POINT SCHEME

Name: Sushna
Rollno: 56
Product Owner:Nowshad C V

Table of Content

1. Description
2. Modules
3. Methodology
4. Developing Environment
5. Future Enhancement
6. Product Backlog
7. User Story
8. Project Plan
9. Sprint Plan
10. Sprint Actual

Description

Authentication is the first line of defence against compromising confidentiality and integrity. Alphanumerical usernames and passwords are the most common method of computer authentication. This method has many drawbacks. Usually people use passwords that can be easily guessed, so that it does not becomes hard to remember. Hence to encounter this problem, researches have developed graphical password authentication methods that use pictures as passwords. Graphical passwords are an alternative to text-based passwords where user is asked to recall an image or parts of an image instead of a word. We are further discussing new and more secure graphical password system called pass points.

In pass points system users can create many points click sequence on a background image. The graphical password is new technique which is more secure than text-based passwords . In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. Users can submit image then he/she can click on the image to create a password then the system pixel tolerance calculates each pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

Modules

1.Registration and Algorithm Implementation

- Defining Click Points
- Algorithm Implementation
- Save to Dataset

2.Authentication

- Selecting clickpoints
- Checking with dataset

3.Comparison and result

- If Data present
- Login

Methodology

The system contain two section : Registration and Main part.

Clicking points for password is done at registration part and checking whether password clicked is correct or not is done at main part.

Algorithm used is Tolerance calculation algorithm , in which tolerance is calculated for the click points.

The algorithm helps to find the nearest place where we clicked and will form a square , inside it any where we can click for our password.

There are four points we have to click and at the fourth click a message box appear as, "Successfully saved ".if we click ok button of message box, a reference image of click points will appear.

The system is more applicable in Digital wallets and Cryptocurrency wallets because it is hard method.

Developing Environment

Hardware specification:

- Processor: i3 Based Computer or higher
- Memory: 1 GB RAM
- Hard Drive: 50 GB
- Monitor
- Internet Connection

Software specification:

- Language :Python
- Front end : Python
- Back end : Python
- Operating system : windows 7 and above
- IDE : PyCham

Future Enhancement

In future it has great scope. It can be used everywhere instead of text-based password . We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many authentication system but they have their own advantages and disadvantages.

This system is more secure and cheap than old methodologies. As well as this system allows more reliable and easily recognizable system to the users. As how we have written over this system can be best alternative to the text password.

Product Backlog

User Story ID	Priority	Size(Hours)	Sprint	Status	Release Date	Release Goal
1	Medium	1	1	completed	28/12/2021	Defining Click Points
2	Medium	2		completed	28/12/2021	Algorithm Implementation
3	High	1		Planned	30/12/2021	Save to Dataset
4	High	2	2	Planned	31/12/2021	Selecting Click Points
5	Medium	2		Planned	15/01/2022	Checking with Dataset
6	Medium	1		Planned	17/01/2022	If Data Present
7	Medium	1	3	Planned	17/01/2022	Login

User Story

User Story ID	As a<type of user>	I want to<perform some task>	So that I can<achieve some goal>
1	User	*Defining Click Points*	Choosing click points inside image
2	User	*Algorithm Implementation*	Click point tolerance calculation algorithm
3	User	*Save to Dataset*	Saving the tolerance data
4	User	*Selecting clickpoints*	Authenticate previously registered click points
5	User	*Checking with dataset*	Checking with tolerance point
6	User	*If Data present*	Checking if data present or not
7	User	Login	If yes login success otherwise login failed

Project Plan

User Story ID	Task Name	Start Date	End Date	Days	Status
1	Sprint1	28/12/2020	28/12/2021	5	completed
2		28/12/2020	28/12/2021		completed
3		30/12/2020	30/12/2021		completed
4	Sprint2	31/12/2020	31/12/2021	2	completed
5		15/01/2022	15/01/2022		completed
6	Sprint3	17/01/2022	17/01/2022	2	completed
7		17/01/2022	17/01/2022		completed

Sprint Plan

Backlog Items(user story)	Completion date	Estimated hrs.	Day 1 Hrs.	Day 2 Hrs.	Day 3 Hrs.	Day 4 Hrs.	Day 5 Hrs.	Day 6 Hrs.	Day 7 Hrs.	Day 8 Hrs.	Day 9 Hrs.	Day 10 Hrs.
1	28/12/2021	5	1	1	0	0	0	0	0	0	0	0
2	28/12/2021	5	1	1	0	0	0	0	0	0	0	0
3	30/12/2021	5	1	1	1	2	0	0	0	0	0	0
4	31/12/2021	5	2	1	2	0	0	0	0	0	0	0
5	15/01/2022	5	1	3	1	0	0	0	0	0	0	0
6	17/01/2022	2	1	1	0	0	0	0	0	0	0	0
7	17/01/2022	3	2	1	0	0	0	0	0	0	0	0
Total		30										

Sprint Actual

Backlog Items(user story)	Completion date	Estimated hrs.	Day 1 Hrs.	Day 2 Hrs.	Day 3 Hrs.	Day 4 Hrs.	Day 5 Hrs.	Day 6 Hrs.	Day 7 Hrs.	Day 8 Hrs.	Day 9 Hrs.	Day 10 Hrs.
1	28/12/2021	3	1	1	1	0	0	0	0	0	0	0
2	28/12/2021	5	1	1	0	0	2	0	0	1	0	0
3	30/12/2021	5	1	0	0	2	0	2	0	0	0	0
4	31/12/2021	2	0	1	0	0	0	0	1	0	0	0
5	15/01/2022	5	2	0	0	1	0	1	0	0	1	0
6	17/01/2022	3	1	0	0	0	1	0	0	0	0	1
7	17/01/2022	2	1	0	0	0	0	1	0	0	0	0
Total		25										

THANK YOU